REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed May 20, 2004. In the Office Action, (i) claims 1-3 were rejected under 35 U.S.C. §102, and (ii) claims 4-33 were rejected under 35 U.S.C. §103. Reconsideration in light of the amendments and remarks made herein is respectfully requested. Claims 1-3, 15, 17, 23, 25, 27 and 29 have been cancelled without prejudice. Claims 4, 6-7, 9-10, 12, 14, 16, 18-19, 21, 24, 26, 28 and 30-33 have been amended.

Rejection Under 35 U.S.C. § 102

Claims 1-3 were rejected under 35 U.S.C. §102(e) as being anticipated by Son, et al. (6,229,895 B1). Although Applicant respectfully traverses the rejection, claims 1-3 have been cancelled without prejudice. Therefore, further discussion of the grounds for traversing this rejection is not warranted at this time.

Applicant respectfully requests withdrawal of the §102(e) rejection.

Rejection Under 35 U.S.C. § 103

Claims 4-33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Son (6,229,895 B1) in view of Wasilewski (US 20040003008A1). Applicants respectfully traverse the rejection because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, when evaluating a claim for determining obviousness, all limitations of the claim must be evaluated. *See In re Fine*, 873 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). According to Figure 3 of Wasilewski, the entitlement management message (315) is loaded into a decryptor (339) being RSA MD5 function. "RSA MD5" is a one-way hashing function where the entitlement management message (315) undergoes a hash operation and the result is compared to a sealed digest within the EMM. *See Col. 8, lines 39-56*. It appears that the private key 337 belonging to DHCT 333 and the public key SP Ku 335 are used for decrypting the EMM (315) and the sealed digest of the EMM, respectively. These keys are parameters used by the decryptor (339) and are not inserted into the EMM (315).

In contrast, independent claims 4, 10, 21 and 32 include a limitation of the "local key" being inserted into the EMM for future access. Wasilewski does not teach or suggest key insertion, and in fact, can be considered to teach away from the claimed invention. Hash functions are not used to insert and subsequently retrieve the inserted data. Hash functions destroy the inserted information and produce a hash result, normally a 128-bit value, which is commonly used for comparison with another hash result.

Applicant respectfully requests the Examiner to contact the undersigned attorney to set up a telephone conference in order to facilitate prosecution of the subject case. The undersigned attorney can be reached at the phone number listed below.

Appl. No. 09/771,363
Amdt. Dated 08/20/2004
Reply to Office Action of May 20, 2004

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 08/20/2004   By

William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING   **FACSIMILE**

☐ *deposited with the United States Postal Service*   ☒ *transmitted by facsimile to the Patent and*
as first class mail in an envelope addressed to: *Trademark Office.*
Commissioner for Patents, PO Box 1450,
Alexandria, VA 22313-1450.

                                                         _____ 08/20/2004
Date: 08/20/2004   *Susan McFarlane*   *Date*